Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (canceled)

2. (currently amended) The method of claim [[1]] 6, further comprising:

for at least one of the plurality of key splits, adding the at least one key split to the encrypted object.

3. (currently amended) The method of claim [[1]] 6, further comprising:

for at least one of the plurality of key splits, adding reference data associated with the at least one key split to the encrypted object.

4. (currently amended) The method of claim [[1]] 6, further comprising retrieving at least one of the plurality of key splits from a storage medium.

5. (previously presented) The method of claim 4, wherein the storage medium is disposed on a smart card.

6. (currently amended) A method of encrypting an object, comprising:

combining a plurality of key splits to generate a cryptographic key;

initializing a cryptographic algorithm with the cryptographic key; and

applying the initialized cryptographic algorithm to the object, to form an encrypted object;

wherein at least one of the plurality of key splits corresponds at least in part to a biometric measurement; and

~~The method of claim 1,~~ wherein combining a plurality of key splits to generate a cryptographic key is performed on a smart card.

7. (currently amended) In a cryptographic system associated with an organization, a method of encrypting an object by a user, comprising:

generating a cryptographic key by combining, on a smart card, an organization split corresponding to the organization, a maintenance split, a random split, a biometric split corresponding to the user, and at least one label split;

initializing a cryptographic algorithm with the cryptographic key;

encrypting the object according to the initialized cryptographic algorithm;

adding combiner data to the encrypted object, wherein the combiner data includes

reference data corresponding to at least one of the at least one label split and the cryptographic algorithm,

name data associated with the organization,

at least one of the maintenance split and a maintenance level associated with the maintenance split, and

the random split; and

storing the encrypted object with the added combiner data.

8. (previously presented) The method of claim 7, further comprising selecting the at least one label split from at least one credential.

9. (previously presented) The method of claim 8, wherein the selected at least one label split is encrypted, the cryptographic key is a first cryptographic key, and the method further comprises:

deriving a second cryptographic key from a user ID associated with the user, a password associated with the user, and at least one of a unique data instance and a random value, and

decrypting the selected at least one label split with the second cryptographic key.

10. (previously presented) The method of claim 8, wherein the at least one credential is retrieved from a memory.

11. (previously presented) The method of claim 10, wherein the memory is disposed on a smart card.

12. (previously presented) The method of claim 8, further comprising generating a time stamp corresponding to a time at which the object was encrypted, wherein the combiner data further includes the time stamp.

13. (previously presented) The method of claim 8, wherein the combiner data further includes a user ID associated with the user.

14. (previously presented) The method of claim 7, further comprising generating a time stamp representing a time at which the object was encrypted, wherein the combiner data further includes the time stamp.

15. (previously presented) The method of claim 7, wherein the combiner data is a header record.

16. (previously presented) The method of claim 7, wherein the combiner data further includes one of a digital signature and a digital certificate.

17. (previously presented) The method of claim 7, wherein the combiner data further includes a digital signature and a digital certificate.

18. (previously presented) The method of claim 7, wherein the cryptographic key is a first cryptographic key, the method further comprising:

generating a second cryptographic key based at least in part on the at least one label split; and

encrypting the random split with the second cryptographic key, prior to adding the combiner data to the encrypted object;

wherein the random split included the combiner data is the encrypted random split.

19. (previously presented) The method of claim 7, further comprising

before adding the combiner data to the encrypted object, encrypting at least a portion of the combiner data with a header split.

20. (previously presented) The method of claim 19, wherein the header split is constant.

21. (canceled)

22. (currently amended) The storage medium of claim ~~21~~ 26, wherein the instructions further include:

for at least one of the plurality of key splits, add the at least one key split to the encrypted object.

23. (currently amended) The storage medium of claim ~~21~~ 26, wherein the instructions further include:

for at least one of the plurality of key splits, add reference data associated with the at least one key split to the encrypted object.

24. (currently amended) The storage medium of claim ~~21~~ 26, wherein the instructions further include:

retrieve at least one of the plurality of key splits from a memory.

25. (previously presented) The storage medium of claim 24, wherein at least a portion of the memory is disposed on a smart card.

26. (currently amended) A storage medium comprising instructions for causing a data processor to encrypt an object, wherein the instructions include:

generate a cryptographic key by combining a plurality of key splits;

initialize a cryptographic algorithm with the cryptographic key; and

apply the initialized cryptographic algorithm to the object to form an encrypted object;

wherein at least one of the plurality of key splits corresponds at least in part to a biometric measurement; and

~~The storage medium of claim 21,~~ wherein the data processor is distributed, and the instruction to generate a cryptographic key is executed at least in part on a smart card.

27. (currently amended) A storage medium comprising instructions for causing a data processor to encrypt an object, wherein the instructions include:

generate a cryptographic key by combining, on a smart card, an organization split corresponding to an organization, a maintenance split, a random split, a biometric split corresponding to the user, and at least one label split;

initialize a cryptographic algorithm with the cryptographic key;

apply the initialized cryptographic algorithm to the object to form an encrypted object;

add combiner data to the encrypted object, wherein the combiner data includes

reference data corresponding to at least one of the at least one label split and the cryptographic algorithm,

name data associated with the organization,

at least one of the maintenance split and a maintenance level corresponding to the maintenance split, and

the random split; and

store the encrypted object with the combiner data for subsequent access.

28. (previously presented) The storage medium of claim 27, wherein the instructions further include select the at least one label split from at least one credential.

29. (previously presented) The storage medium of claim 28, wherein the selected at least one label split is encrypted, the cryptographic key is a first cryptographic key, and the instructions further include:

derive a second cryptographic key from a user ID associated with a user, a password associated with the user, and at least one of a unique data instance and a random value; and

decrypt the selected at least one label split with the second cryptographic key.

30. (previously presented) The storage medium of claim 28, wherein the instructions further include:

retrieve at least one credential from a memory.

31. (previously presented) The storage medium of claim 30, wherein the memory is disposed on a smart card.

32. (previously presented) The storage medium of claim 28, wherein the instructions further include generate a time stamp corresponding to a time at which the object was encrypted, wherein the combiner data further includes the time stamp.

33. (previously presented) The storage medium of claim 28, wherein the combiner data further includes a user ID associated with the user.

34. (previously presented) The storage medium of claim 27, wherein the instructions further include generate a time stamp corresponding to at which the object was encrypted, wherein the combiner data further includes the time stamp.

35. (previously presented) The storage medium of claim 27, wherein the combiner data is a header record.

36. (previously presented) The storage medium of claim 27, wherein the combiner data further includes one of a digital signature and a digital certificate.

37. (previously presented) The storage medium of claim 27, wherein the combiner data further includes a digital signature and a digital certificate.

38. (previously presented) The storage medium of claim 27, wherein the cryptographic key is a first cryptographic key, and the instructions further include:

generate a second cryptographic key based at least in part on the at least one label split; and

encrypt, with the second cryptographic key, the random split, prior to executing the instruction to add the combiner data to the encrypted object;

wherein the random split included in the combiner data is the encrypted random split.

39. (previously presented) The storage medium of claim 27, wherein the instructions further include

prior to executing the instruction to add the combiner data to the encrypted object, encrypt at least a portion of the combiner data with a header split;

40. (previously presented) The storage medium of claim 39, wherein the header split is constant.

41. (currently amended) The method of claim [[1]] 6, wherein combining the plurality of key splits includes applying a non-linear function to the plurality of key splits.

42. (previously presented) The method of claim 41, wherein the cryptographic key is a single-integer cryptographic key.

43. (currently amended) The method of claim [[1]] 6, wherein the key splits are provided by at least one of a policy manager and a credentials manager.

44. (currently amended) The method of claim [[1]] 6, wherein the cryptographic algorithm is a symmetrical algorithm.

45. (currently amended) The method of claim [[1]] 6, wherein the cryptographic key is a session key.

46. (previously presented) The method of claim 7, wherein combining the organization split, the maintenance split, the random split, and the at least one label split includes applying a non-linear function to the splits

47. (previously presented) The method of claim 46, wherein the cryptographic key is a single-integer cryptographic key.

48. (previously presented) The method of claim 7, wherein the organization split, the maintenance split, the random split, and the at least one label split are provided by at least one of a policy manager and a credentials manager.

49. (previously presented) The method of claim 7, wherein the cryptographic algorithm is a symmetrical algorithm.

50. (previously presented) The method of claim 7, wherein the cryptographic key is a session key.

51. (currently amended) The storage medium of claim ~~21~~ 26, wherein combining the plurality of key splits includes applying a non-linear function to the plurality of key splits.

52. (previously presented) The storage medium of claim 51, wherein the cryptographic key is a single-integer cryptographic key.

53. (currently amended) The storage medium of claim ~~21~~ 26, wherein the key splits are provided by at least one of a policy manager and a credentials manager.

54. (currently amended) The storage medium of claim ~~21~~ 26, wherein the cryptographic algorithm is a symmetrical algorithm.

55. (currently amended) The storage medium of claim ~~21~~ 26, wherein the cryptographic key is a session key.

56. (previously presented) The storage medium of claim 27, wherein combining the organization split, the maintenance split, the random split, and the at least one label split includes applying a non-linear function to the splits.

57. (previously presented) The storage medium of claim 56, wherein the cryptographic key is a single-integer cryptographic key.

58. (previously presented) The storage medium of claim 27, wherein the organization split, the maintenance split, the random split, and the at least one label split are provided by at least one of a policy manager and a credentials manager.

59. (previously presented) The storage medium of claim 27, wherein the cryptographic algorithm is a symmetrical algorithm.

60. (previously presented) The storage medium of claim 27, wherein the cryptographic key is a session key.